CloudFlare tackles lost SSL key risk with Keyless SSL

September 19 2014, by Nancy Owano

Organizations looking for and concerned about optimal security protection are the targets of a new service announced by San Francisco-based CloudFlare. The offering is called Keyless SSL. CloudFlare explained that "An SSL key is the data that allows an organization to establish a secure connection with the customers that connect to it. It is also the data that lets an organization establish its identity." Here is the heartache. If you have an organization private SSL key, you can authenticate as if you were it. You can spoof identity and intercept traffic. "If, say, a media organization loses an SSL key, it's a very bad day," blogged CEO Matthew Prince. "If a financial institution loses one,

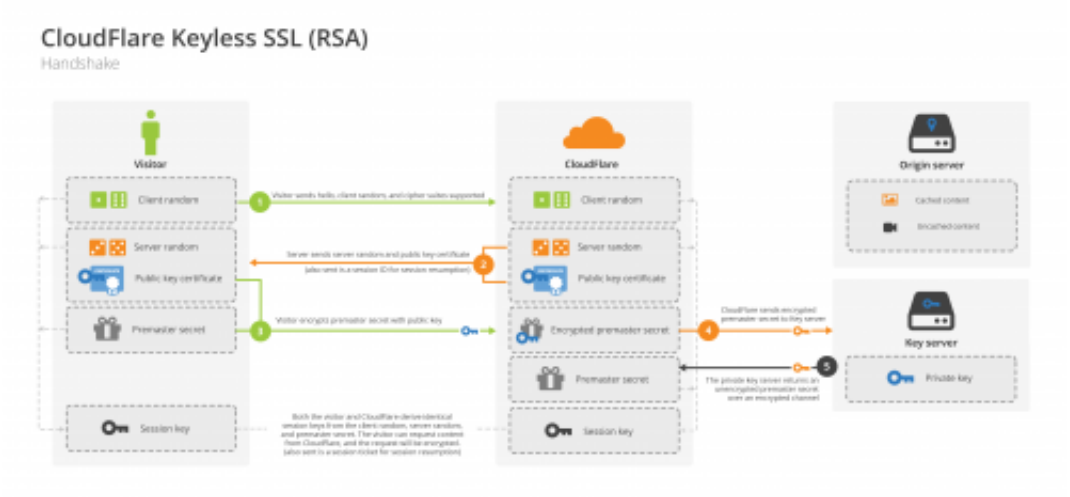
it's a nightmare." Serdar Yegulalp, a senior writer at InfoWorld, said that, "With a conventional SSL system, the private key used to sign all sessions is normally held on the same public-facing server used to fulfill Web traffic. The potential dangers of this system were dramatized by the Heartbleed bug, where private key information could be leaked out."

CloudFlare on Thursday announced its new service, Keyless SSL, designed for organizations taking to the idea of defending themselves against distributed denial of service attacks on their websites without having to turn over private encryption keys. They will use CloudFlare's network of 28 data centers worldwide. As TechCrunch noted, this process allows companies to use the cloud while maintaining complete control of the SSL key. Sean Gallagher of Ars Technica wrote, "Keyless SSL breaks the encryption 'handshake' at the beginning of a Transport Layer Security (TLS) Web session, passing part of the data back to the organization's data center for encryption."

The system was several years in development, with the CloudFlare team working on ways to allow banks to hold onto their private keys. "The story begins on a Saturday morning, in the Fall of 2012," said Prince, "almost exactly two years ago. I got a call on my cell phone that woke me. It was a man who introduced himself as the Chief Information Security Officer (CISO) at one of the world's largest banks. 'I got your number from a reporter,' he said. 'We have an incident. Could you and some of your team be in New York Monday morning? We'd value your advice.' We were a small startup. Of course we were going to drop everything and fly across the country to see if we could help."

Jack Clark commented in Bloomberg on Thursday that security company CloudFlare's new product "may raise its prominence among banks faced with mounting cyberattacks." By using Keyless SSL, wrote Gallagher in Ars Technica, "CloudFlare will be able to put servers in less secure data centers without leaving keys at risk. Since everything is in memory,

everything in a remote data center disappears when the servers are rebooted. The master encryption keys are never put at risk."



"Announcing Keyless SSL: All the Benefits of CloudFlare Without Having to Turn Over Your Private SSL Keys," blogged Prince on Thursday, adding "welcome to the no hardware world."

More information: blog.cloudflare.com/announcing … ur-private-ssl-keys/

Citation: CloudFlare tackles lost SSL key risk with Keyless SSL (2014, September 19) retrieved 16 April 2024 from https://techxplore.com/news/2014-09-cloudflare-tackles-lost-ssl-key.html